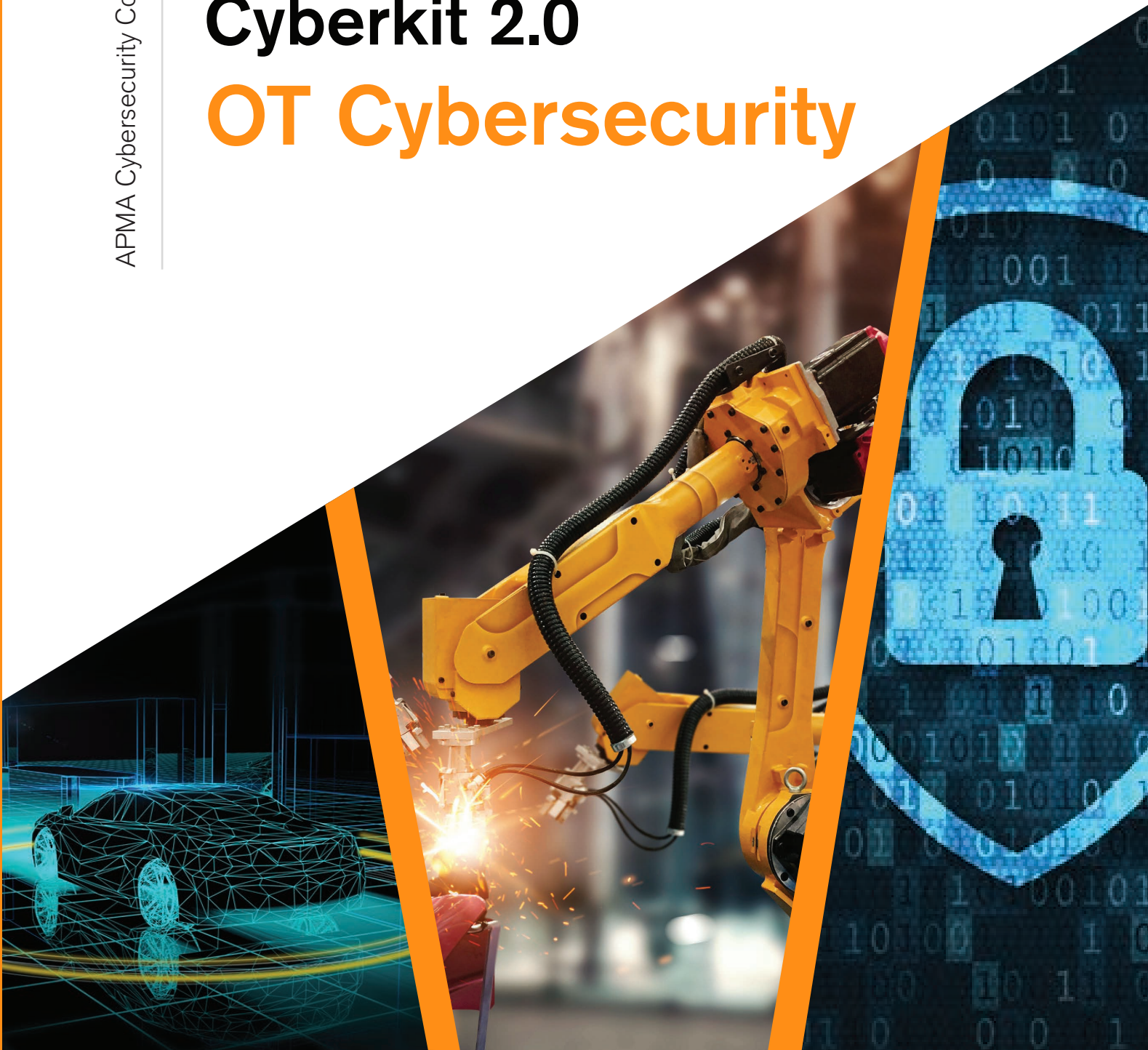


APMA Cybersecurity Committee

Cyberkit 2.0

OT Cybersecurity



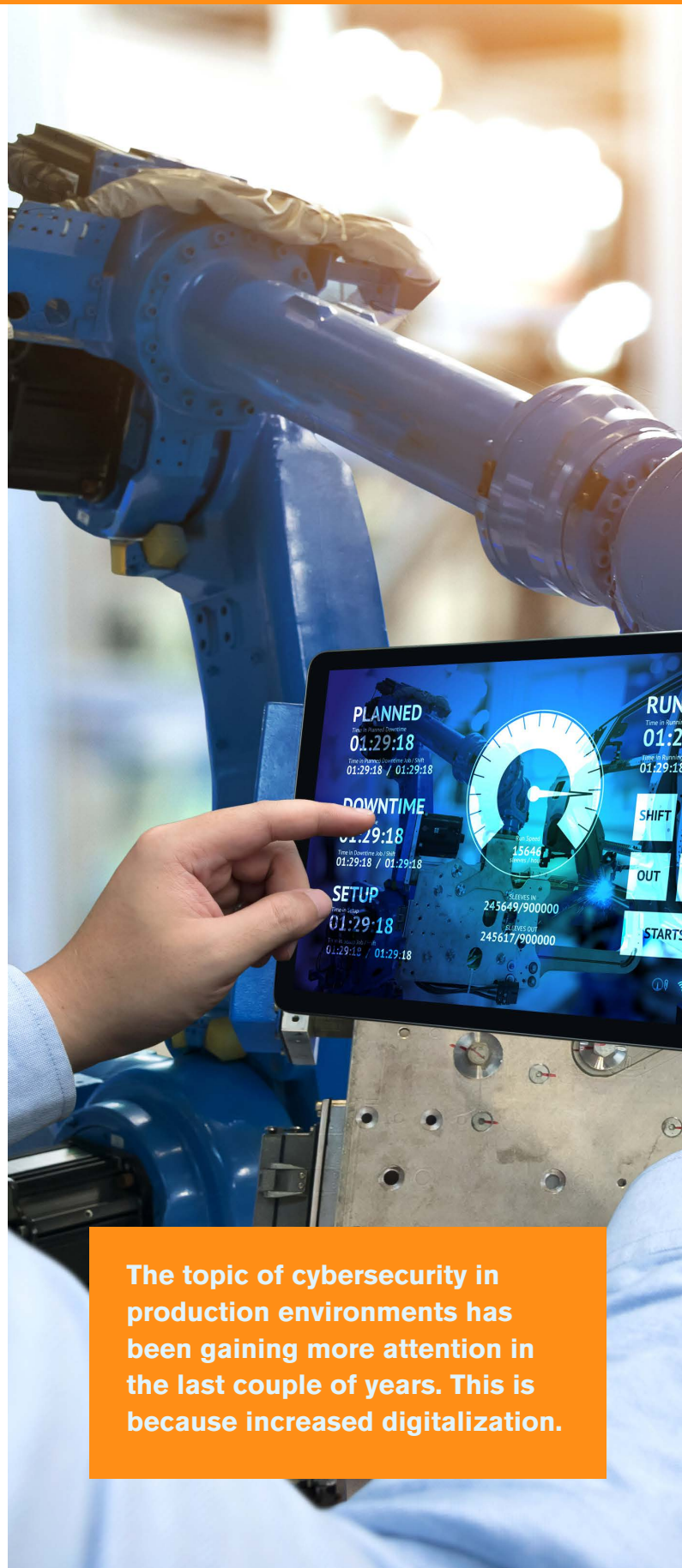


Introduction

CyberKit 1.0 provided, among other things, an overview of Cybersecurity Governance Frameworks, in particular NIST's widely adopted general Cybersecurity Framework and the new ISO 21434 standard for cybersecurity engineering for road vehicles.

The latter provides requirements to ensure that information and communication technologies designed into vehicles are as secure as possible. In this module, we will provide an introductory discussion of a complementary but equally important topic: protecting the industrial production sites where the parts and components for such vehicles are manufactured. This is often referred to as Operational Technology (OT) Cybersecurity.

The topic of cybersecurity in production environments has been gaining more attention in the last couple of years. This is because increased digitalization of those environments and their related processes – often captured by terms such as “Industry 4.0” or “Industrial Internet of Things” – not only offers the prospect of productivity gains but also at the same time increases the vulnerability to cyber-attacks. In addition, recent years have seen an increasing number of industrial facilities attacks, often with significant physical and/or financial impact.



The topic of cybersecurity in production environments has been gaining more attention in the last couple of years. This is because increased digitalization.

How OT environments are different

When securing OT environments such as a manufacturing plant, it is essential to consider some significant differences compared to traditional IT systems found in typical office environments.

While IT security traditionally focuses on the CIA triad of Confidentiality, Integrity and Availability of data, in OT environments, the focus is typically on SRA, that is, Safety, Reliability and Availability of equipment and

machinery. While modern IT technologies are more and more becoming part of OT environments – often referred to as “IT-OT convergence” – there are still some significant differences, as shown in the table below.

IT Security		Industrial Security
3-5 years	Asset lifecycle	15-25 years
✓ Fairly homogeneous	✓ Heterogeneity	✓ Heterogeneous
✓ Windows (10 or 7) or Linux		✓ Wide variety of Windows systems (95 to 10), Embedded OS, PLC OS
✓ IP/TCP standard communication		✓ Many proprietary communication protocols
✓ Tolerated	✓ Downtime	✓ Unacceptable, except as scheduled maintenance
✓ Frequently runs as background process	✓ Software updates	✓ Only possible as part of scheduled maintenance

The Importance of a Holistic Approach to Securing a Production Plant

Given the complexity of modern manufacturing environments, it is prudent to take a holistic approach to design the security architecture and features.

A practical approach to this is using a defence-in-depth model, where security features are designed and implemented for three different zones of the overall plant environment, including the facilities' physical security. An excellent approach to design specific cybersecurity controls when implementing such a

model is to use international standards and guidelines. Arguably the two most well-known ones for industrial security are the IEC/ISA 62443 standards and the NIST Guide to Industrial Control Systems security. References are provided below.



Some first steps to get started

Systematically applying a comprehensive standard such as IEC 62443 in a manufacturing plant is a significant undertaking in time commitment and expert resources.

Depending on the maturity of the existing cybersecurity program in the organization, it might be best to start with some first concrete steps to achieve some early successes. Such steps can include:

- ✓ **OT asset discovery: ensure full transparency into all relevant OT assets that have a network connection.**
- ✓ **Ensure proper configuration and patch management of all IT and OT assets in the manufacturing environment. Assets that cannot be patched because they contain legacy software or because of operational constraints might require superior protection, e.g. through dedicated firewalls**
- ✓ **Manage physical access to assets and secure remote access. Having proper authentication and authorization procedures in place is key**
- ✓ **Implement application whitelisting**




Moving beyond basic protection concepts

In the last 5 – 10 years, the sophistication of cybersecurity attacks by highly organized cybercrime actors has increased tremendously.

A whole shadow economy of “Cybercrime-as-a-Service” has developed, driven by billions of dollars in profit from the theft of valuable data and ransomware payments. Defending against these advanced threats requires the ability to detect intrusions in real-time through monitoring of networks and endpoints of both OT systems and IT systems deployed in the OT environment.

Furthermore, strong incident response capabilities are needed to deal with intrusions once they have been detected. Most small to medium-sized organizations will likely require an external partner’s assistance, such as a consulting company specializing in OT cybersecurity or a managed security services provider to deploy such capabilities.



“Cybercrime-as-a-Service” has developed, driven by billions of dollars in profit from the theft of valuable data and ransomware payments.

Acknowledgements

OT Cybersecurity module:



Flavio Volpe

President, APMA



Colin Dhillon

Chief Technical Officer, APMA

The Automotive Parts Manufacturers' Association (APMA) of Canada President and CTO would like to thank the cybersecurity committee members for their continued efforts to provide leadership and a global voice on the topic of automotive cybersecurity, privacy and cyber safety. The work you have all undertaken is having a positive impact in the complete auto ecosystem.

Mr. Oliver Winkler

Business Leader,
Strategy & Innovation
Siemens



We would like to acknowledge Mr. Oliver Winkler, Business Leader, Strategy & Innovation at Siemens Canada for leading the development of the OT Cybersecurity module for Cyberkit 2.0.

The APMA would also like to thank the members of its cybersecurity committee for their continued support and ongoing efforts.

Catherine Bertheau - Cyber Solutions Business Dev Lead - Aon
Sumit Bhatia – Director, Communications & Knowledge Mobilization -- Ryerson Cybersecure Catalyst
Todd Bielarczyk - Intelligence Officer - CSIS
Olivier Charron – Microsoft Canada
Sarah Chippure – Senior Policy Analyst - Transport Canada
Ali Dehghantanha – Director – Cyber Science Lab – University of Guelph
Trish Dyl – Director of Partnerships – Ryerson Cybersecure Catalyst
Peter Elliot – Global Information Security Officer – Magna International
John Esvelt – Chief Risk Officer - Dentons
Sebastian Fischmeister – Professor – University of Waterloo
John Heaton – Partner, Cybersecurity - KPMG
Ganesh Iyer - CIO & VP of Eng. - Martinrea
Marc Kneppers - Chief Security Architect – Telus Communications
Philip Lafrance – Standards Manager - Isara
Kevin Magee – Chief Security and Compliance Officer - Microsoft Canada
Siddhartha Parti -Global Director IT, Infrastructure & Ops – Woodbridge
Ken Schultz – General Manager - Escript
Jazz Singh – Cybersecurity, IT & Risk – TD Bank
Cara Wolf – Founder & CEO – Ammolite Analytix
John Wright – Founder & Chairman - JPOM

References:

Below are additional resources for OT Cybersecurity

Primer for Cybersecurity in Industrial Automation

A free e-book from the International Society of Automation (ISA) and Siemens, available for download at:

<https://new.siemens.com/global/en/products/services/digital-enterprise-services/industrial-security-services.html>

IEC 62443 – a series of standards to secure industrial communication networks and industrial automation and control systems

<https://etech.iec.ch/issue/2020-04/iec-62443-standards-a-cornerstone-of-industrial-cyber-security>

NIST SP 800-82 Guide to Industrial Control Systems (ICS) Security

<https://csrc.nist.gov/publications/detail/sp/800-82/rev-2/final>

The background of the slide is a warm, orange-toned photograph of an industrial setting. On the left, a yellow robotic arm is visible, with its joints and end effector in focus. On the right, a person's hand is holding a tablet computer, which displays a control interface with various icons and graphs. The overall scene suggests a connection between human operators and automated industrial systems.

Module: OT Cybersecurity

